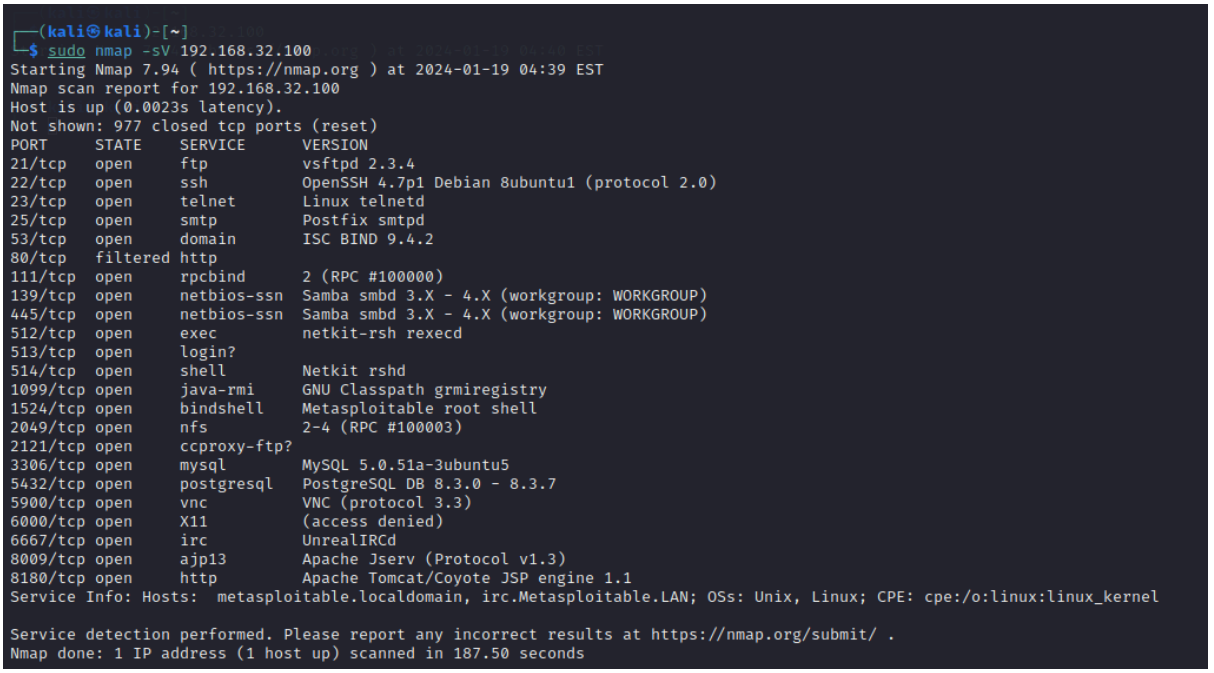
Traccia

https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/

Utilizzare alcuni di questi strumenti per raccogliere informazioni sulla macchina metasploitable e produrre un report.

Nel report indicare sopra l'esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate

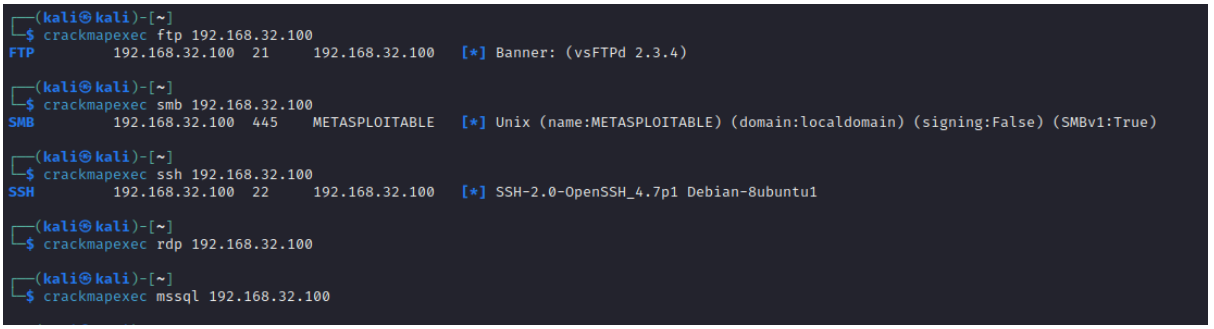
1. Scansione con nmap -sV



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.32.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 04:39 EST
Nmap scan report for 192.168.32.100
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 2.3.4
22/tcp   open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open     telnet       Linux telnetd
25/tcp   open     smtp         Postfix smtpd
53/tcp   open     domain       ISC BIND 9.4.2
80/tcp   filtered http
111/tcp  open     rpcbind      2 (RPC #100000)
139/tcp  open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open     exec         netkit-rsh rexecd
513/tcp  open     login?
514/tcp  open     shell        Netkit rshd
1099/tcp open     java-rmi     GNU Classpath grmiregistry
1524/tcp open     bindshell    Metasploitable root shell
2049/tcp open     nfs          2-4 (RPC #100003)
2121/tcp open     ccproxy-ftp?
3306/tcp open     mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp open     postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc          VNC (protocol 3.3)
6000/tcp open     X11          (access denied)
6667/tcp open     irc          UnrealIRCd
8009/tcp open     ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open     http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 187.50 seconds
```

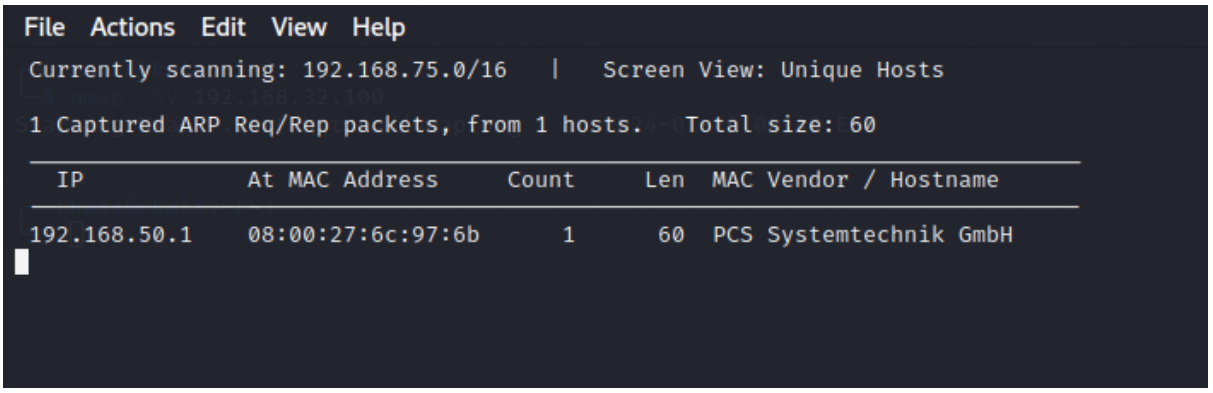
Questo tipo di scansione ci riporta tutti i servizi attivi della macchina scansionata e la loro versione che potremmo sfruttare per aver più informazioni sulle vulnerabilità.
Un esempio è la porta 21/tcp versione vsftpd 2.3.4 che facendo una piccola ricerca con google riusciamo a trovare le sue vulnerabiltà.

2. Scansione con crackmapexec



```
┌──(kali㉿kali)-[~]
└─$ crackmapexec ftp 192.168.32.100
FTP         192.168.32.100  21     192.168.32.100   [*] Banner: (vsFTPd 2.3.4)

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.32.100
SMB         192.168.32.100  445    METASPLOITABLE   [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True)

┌──(kali㉿kali)-[~]
└─$ crackmapexec ssh 192.168.32.100
SSH         192.168.32.100  22     192.168.32.100   [*] SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

┌──(kali㉿kali)-[~]
└─$ crackmapexec rdp 192.168.32.100

┌──(kali㉿kali)-[~]
└─$ crackmapexec mssql 192.168.32.100
```

3 Scansione con Netdiscover



Tra le info di queste tool notiamo il vendor della Nic riconosciuto tramite l'indirizzo MAC.